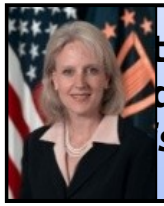
Program Protection and Cybersecurity

Melinda Reed
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

2016 Product Support Manager's Workshop
Fort Belvoir, Virginia | April 5, 2016

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

DASD, Systems Engineering



ting Deputy Assistant Secretary of Defense
d Principal Deputy, Systems Engineering
sten Baldwin

Homeland Defense Capability Development
Robin Hicks

Major Program Support
ames Thompson

ngineering Enterprise
obert Gold

Supporting USD(AT&L) Decisions with Independent Engineering Expertise

- **Engineering Assessment / Mentoring of Major Defense Programs**
- **Program Support Assessments**
- **Overarching Integrated Product Team and Defense Acquisition Board Support**
- **Systems Engineering Plans**
- **Systemic Root Cause Analysis**
- **Development Planning/Early SE**
- **Program Protection**

Leading Systems Engineering Practice in DoD and Industry

- **Systems Engineering Policy and Guidance**
- **Technical Workforce Development**
- **Specialty Engineering (System Safety, Reliability and Maintainability, Quality, Manufacturing, Producibility, Human Systems Integration)**
- **Security, Anti-Tamper, Counterfeit Prevention**
- **Standardization**

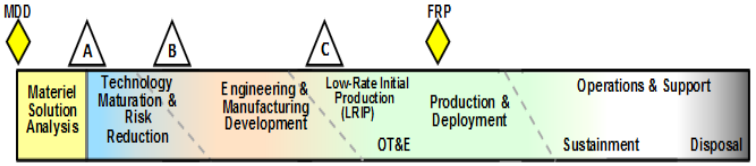
Providing technical support and systems engineering leadership and oversight to USD(AT&L) in support of planned and ongoing acquisition programs

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

Ensuring Confidence in Defense Systems

- ***Threat:***
  - Adversary who seeks to exploit vulnerabilities to:
    - Acquire program and system information;
    - Disrupt or degrade system performance;
    - Obtain or alter US capability
- ***Vulnerabilities:***
  - All systems, networks, and applications
  - Intentionally implanted logic (HW/SW)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
  - Controlled defense information resident on, or transiting supply chain networks
  - Loss or sale of US capability that provides a technological advantage
- ***Consequences:***
  - Loss of data; system corruption
  - Loss of confidence in critical warfighting capability; mission impact
  - Loss of US capability that provides a technological advantage

Access points are throughout the acquisition lifecycle…

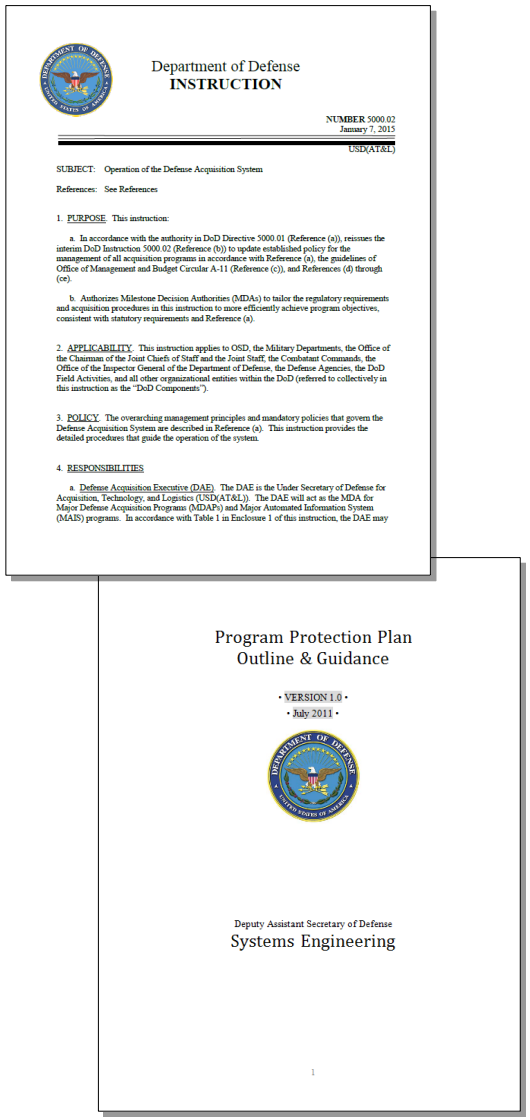


…and across numerous supply chain entry points

- Government
- Prime, subcontractors
- Vendors, commercial parts manufacturers
- 3rd party test/certification activities

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

Program Protection in DoDI 5000.02


Department of Defense
INSTRUCTION

NUMBER 5000.02
January 7, 2015
USD(AT&L)

SUBJECT: Operation of the Defense Acquisition System

References: See References

1. PURPOSE. This instruction:

a. In accordance with the authority in DoD Directive 5000.01 (Reference (a)), reissues the interim DoD Instruction 5000.02 (Reference (b)) to update established policy for the management of all acquisition programs in accordance with Reference (a), the guidelines of Office of Management and Budget Circular A-11 (Reference (c)), and References (d) through (ee).

b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

2. APPLICABILITY. This instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

3. POLICY. The overarching management principles and mandatory policies that govern the Defense Acquisition System are described in Reference (a). This instruction provides the detailed procedures that guide the operation of the system.

4. RESPONSIBILITIES

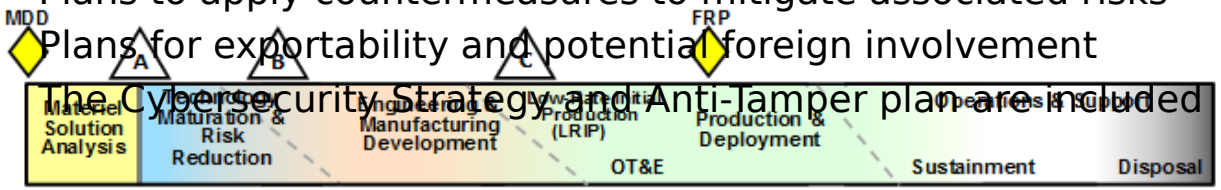
a. Defense Acquisition Executive (DAE). The DAE is the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)). The DAE will act as the MDA for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs. In accordance with Table 1 in Enclosure 1 of this instruction, the DAE may

Program Protection Plan
Outline & Guidance

• VERSION 1.0 •
• July 2011 •

Deputy Assistant Secretary of Defense
Systems Engineering

- **DoD considers SSE a critical discipline of SE. To further establish SSE, DoD has focused on integrating SSE into SE policy, contracts and workforce education.**
- **System Security Engineering is accomplished in the DoD through program protection planning (PPP)**
- **DoDI 5000.02 requires program managers to employ system security engineering practices and prepare a Program Protection Plan to manage the security risks to critical program information, mission-critical functions and information**
- **Program managers will describe in their PPP:**
  - Critical Program Information, mission-critical functions and critical components, and information security threats and vulnerabilities
  - Plans to apply countermeasures to mitigate associated risks
  - Plans for exportability and potential foreign involvement
  - The Cybersecurity Strategy and Anti-Tamper plan are included



Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

Cybersecurity in Acquisition

- **Acquisition workforce must take responsibility for the cybersecurity of their programs from earliest research and technology development through system concept, design, development, test and evaluation, production, fielding, sustainment, and disposal**

- **Scope of program cybersecurity includes:**
  - Program information Data about acquisition, personnel, planning, requirements, design, test data and support data for the system. Also includes data that alone might not be unclassified or damaging, but in combination with other information could allow an adversary to compromise, counter, clone, or defeat warfighting capability
  - Organizations and Personnel Government program offices, prime and subcontractors, along with manufacturing, testing, depot and training organizations
  - Networks Government and Government support activities, unclassified and classified networks, contractor unclassified and classified networks, and interfaces among Government and contractor networks
  - Systems and Supporting Systems The system being acquired, system interfaces, and associated training, testing, manufacturing, logistics, maintenance and other support systems

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

What Are We Protecting?

Program Protection Planning

DoDI 5000.02

DoDM 5200.01, Vol. 1-4

DoDM 5200.45

DoDI 8500.01

DoDI 5200.39

DoDI 5200.44

DoDI 5230.24

DoDI 8510.01

Technology

What: A capability element that contributes to the warfighters' technical advantage (CPI)

Who Identifies: System Engineers with CI/Intel and Security SME support

ID Process: CPI Identification

Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence (CI) assessments

Countermeasures: Anti-Tamper, Classification, Exportability

Components

What: Mission-critical elements and components

Who Identifies: System Engineers, Logisticians

ID Process: Criticality Analysis

Threat Assessment: Defense Intelligence Agency Threat Analysis Center

Countermeasures: SCRM, Cybersecurity, Anti-counterfeits, software assurance, Trusted Foundry, etc.

Information

What: Information about applications, processes, capabilities and end-items

Who Identifies: All

ID Process: CPI identification, criticality analysis, and classification guidance

Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence assessments

Countermeasures: Cybersecurity, Classification, Export Controls, Security, etc.

Protecting Warfighting Capability Throughout the Lifecycle

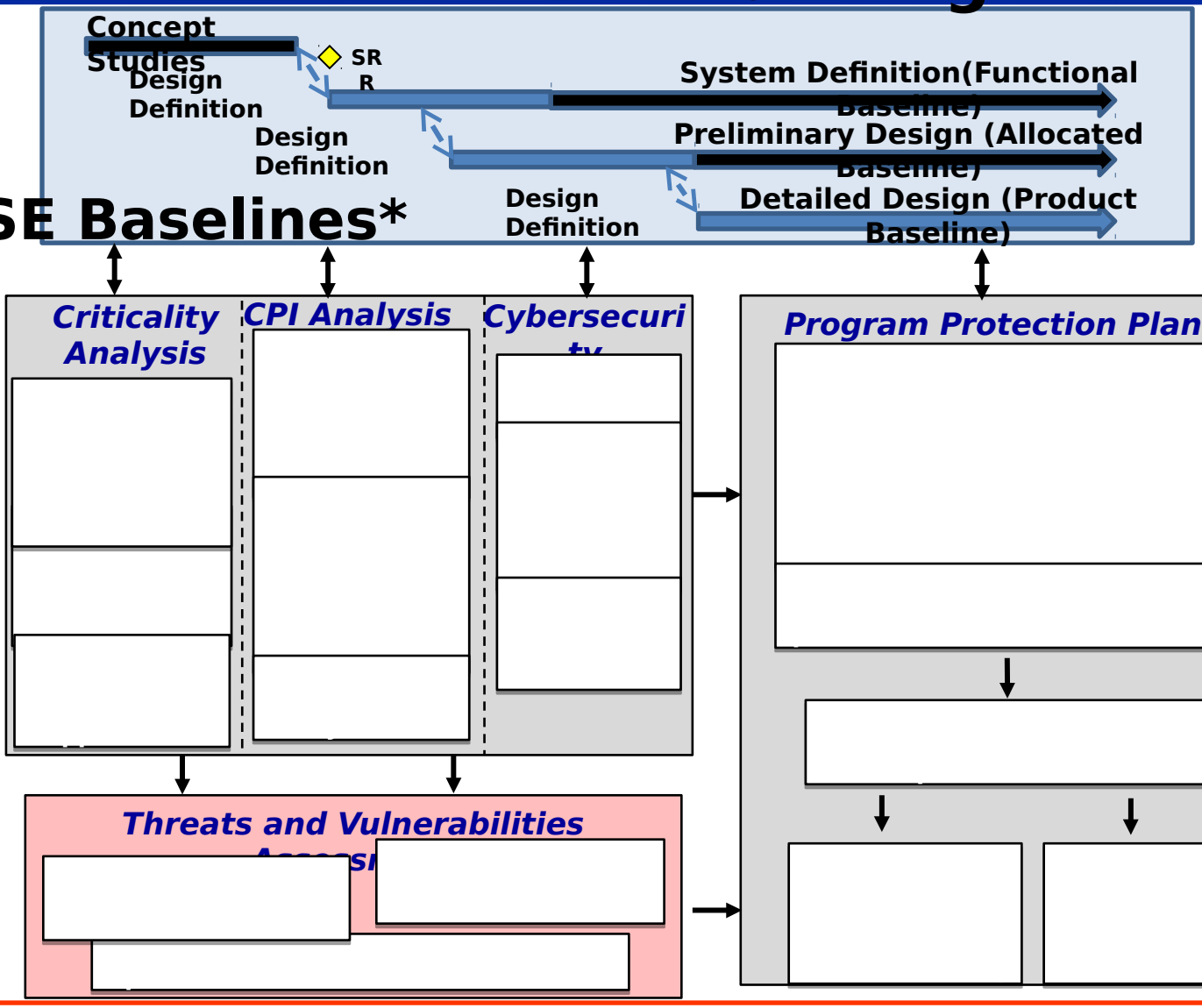
and loss of CPI

http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

from our adversaries

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

Systems Security Engineering Integrates Program Protection Planning



Protection measures are identified and integrated into technical baselines, iteratively informed by and informing the maturing design.

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

Spectrum of Program Protection Risks to Consider

Quality Escape

inadequacy introduced either through mistake or negligence during design, production, and post-production handling resulting in the introduction of deficiencies, vulnerabilities, and degraded life-cycle

Reliability Failure

Mission failure in the field due to environmental factors unique to military and aerospace environment factors such as particle strikes, device aging, hot-spots, electro-magnetic pulse, etc.

Fraudulent Product

Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.

Malicious Insertion

malicious hard/soft coding, or defect to enable physical attacks or cause mission failure; includes logic bombs, Trojan 'kill switches' and backdoors for unauthorized control and

Reverse Engineering

Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.

Information Losses

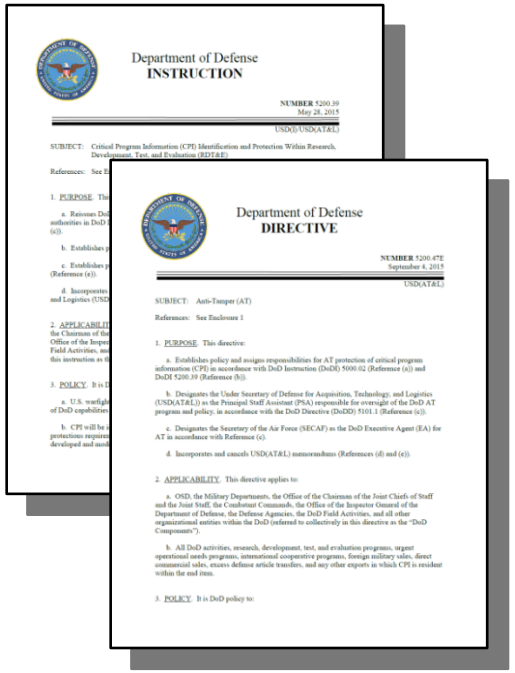
Stolen data provides potential adversaries extraordinary insight into US defense and industrial capabilities and allows them to save time and expense in developing similar capabilities.

DoD Program Protection focuses on risks posed by malicious actors

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

CPI Policy Updates

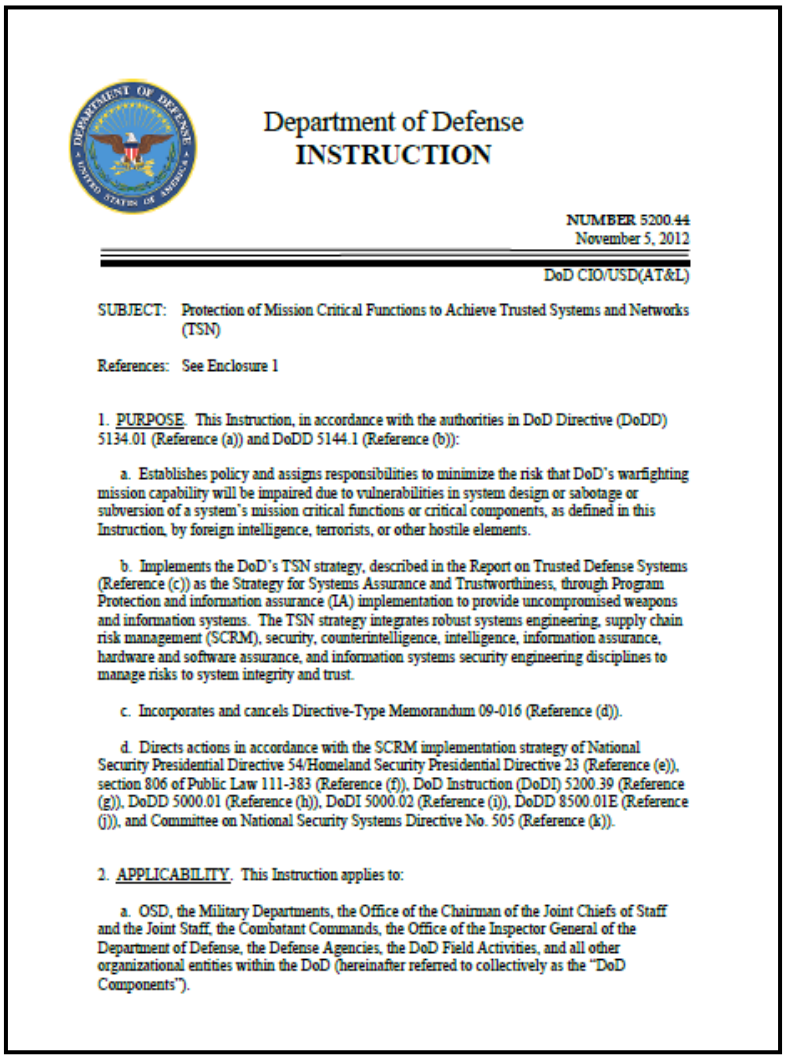
- **CPI and AT Policy Updates**
  - ***DoDI 5200.39, Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E):*** Revises the CPI definition, requires CPI identification early and throughout the program, and emphasizes horizontal identification and protection
  - ***DoDD 5200.47E, Anti-Tamper:*** Designates the Secretary of the AF as the Executive Agent for Anti-Tamper and establishes requirements for AT planning, implementation, and evaluation.



- **Revised definition of CPI has been scoped to focus only on those elements that provide a capability advantage and reside on the end-item (system or supporting systems)**
  - **"U.S. capability elements that contribute to the warfighters' technical advantage, which if compromised, undermines U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment."**

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

Trusted Systems and Networks DoD Instruction 5200.44



Department of Defense
INSTRUCTION

NUMBER 5200.44
November 5, 2012

DoD CIO/USD(AT&L)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.1 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and information assurance (IA) implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoD Instruction (DoDI) 5200.39 (Reference (g)), DoDD 5000.01 (Reference (h)), DoDI 5000.02 (Reference (i)), DoDD 8500.01E (Reference (j)), and Committee on National Security Systems Directive No. 505 (Reference (k)).

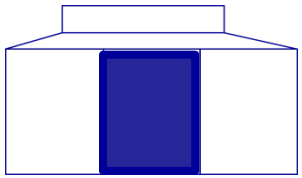
2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

- **Implements the DoD's Trusted Systems and Networks (TSN) strategy**
- **Manage risk of mission-critical function and component compromise throughout lifecycle of key systems by utilizing**
  - Criticality Analysis as the systems engineering process for risk identification
  - Countermeasures: Supply chain risk management, software assurance, secure design patterns
  - Intelligence analysis to inform program management
- **Codify trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)**
- **Document planning and accomplishments in program**

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

Joint Federated Assurance Center



- **JFAC is a federation of DoD software and hardware assurance (SwA/HwA) capabilities and capacities**
  - To support programs in addressing current and emerging threats and vulnerabilities
  - To facilitate collaboration across the Department and throughout the lifecycle of acquisition programs
  - To maximize use of available resources
  - To assess and recommend capability and capacity gaps to resource

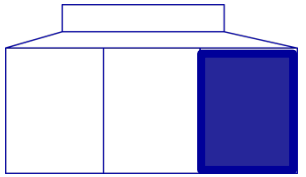
- **Innovation of SW and HW inspection, detection, analysis, risk assessment, and remediation tools and techniques to mitigate risk of malicious insertion**
  - R&D is key component of JFAC operations
  - Focus on improving tools, techniques, and procedures for SwA and HwA to support programs

- **Federated Organizations**
  - Army, Navy, AF, NSA, DMEA DISA, NRO, MDA laboratories and engineering support organizations; Intelligence Community and Department of Energy

The mission of JFAC is to support programs with SwA and HwA needs

Distribution Statement A - Approved for public release by DOPSR. Distribution is unlimited.

Safeguarding Covered Defense Information Contract Regulation



DFARS 252.204-7012 - amended on Aug 26, 2015 (80 FR 51739), to implement section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013; section 1632 of the NDAA for FY 2015; and DoD policies and procedures with regard to cloud computing.

Purpose:

Establish minimum requirements for DoD unclassified covered defense information, which includes information with established marking requirements, e.g. controlled technical information, on contractor information systems

Requires:

Contractor compliance with security requirements in the NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,"

Flow Down only to Subcontractors where their efforts will involve covered defense information or where they will provide operationally critical support.

Contractors report cyber incident and compromises affecting covered defense information and submission of discovered malware

Contractor actions to support DoD damage assessment as needed

DoD published a second Interim Rule on Dec 30, 2015 incorporating flexibilities and accommodations we can provide without compromising the security of Defense information on contractor information systems.

Distribution Statement A. Approved for Public Release by DOPSR. Distribution is unlimited.

Incorporating Program Protection into Acquisition Workforce Training

- **Effective program protection planning is enabled by qualified, trained personnel**
  - **Two program protection courses are currently in development**
  - **First course (ACQ 160) is expected to be available in FY16**
  - **Continuous learning modules on specific security topics**

Defense Acquisition University

- **ACQ 160: Program Protection Overview**
  - Provides an overview of program protection concepts, policy and processes
  - Intended for the entire Acquisition Workforce, with focus on ENG and PM
- **ENG 260: Program Protection Practitioner Course**
  - Intended for Systems Engineers and System Security Engineers
  - Focuses on application of program protection concepts and processes
- **CLMs for Supply Chain Risk Management and Software Assurance**

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

Questions

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.